<u>**REMARKS**</u>

Please reconsider the application in view of the above amendments and the following remarks. Applicant thanks the Examiner for carefully considering this application.

Disposition of Claims

Claims 1-9, 11-20, and 22-35 were pending in the present patent application. By way of this reply, claim 24 has been cancelled without prejudice or disclaimer. Accordingly, claims 1-9, 11-20, 22, 23, and 25-35 are pending in the present invention. Claims 1, 17, 18, 34, and 35 are independent. The remaining claims depend, either directly or indirectly, from claims 1 and 18.

Claim Amendments

Claims 1, 17, 18, 34, and 35 have been amended to include the limitations of now-cancelled dependent claim 24. Claims 18, 27, 28, and 34 have been amended for clarification. No new matter has been introduced by way of these amendments as support for these amendments may be found, for example, in paragraphs [0037], [0038], and Figures 4 and 7 of the published Specification.

Drawings

Applicant respectfully requests the Examiner acknowledge the drawings filed on March 22, 2002, and indicate whether they are acceptable.

Rejections under 35 U.S.C. §101

Claims 18-20 and 22-34 stand rejected under 35 U.S.C. §101 for being directed towards non-statutory subject matter. By way of this reply, claim 24 has been cancelled and

thus the rejection is moot as to that claim. As for the remaining claims, for the reasons set forth below, this rejection is respectfully traversed.

Independent claim 18 has been amended to recite, in part, "a computer implemented method" and "wherein the stored encrypted serialized file enables the key and the key encryption key to be securely stored on a server." Independent claim 34 has been amended to include similar limitations. Therefore, amended independent claims 18 and 34 recite the use of both data and an algorithm to produce a concrete, tangible, and useful result (*e.g.*, an encrypted serial file accessible only to those with the key encryption key and enabled to be securely stored on any server). Thus, Applicant asserts claim 18-20, 22, 23, and 25-35 are directed towards statutory subject matter and have utility. Accordingly, withdrawal of this rejection is respectfully requested.

Rejections under 35 U.S.C §112

Claims 1-20 and 22-35 are rejected under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and claim the subject matter which applicant regards as the invention. Specifically, the Examiner asserts the term "is active" in claims 1, 17, 18, 34, and 35 is a relative term which renders the claim indefinite. (*See* Office Action dated October 24, 2005 at page 3). The Examiner asserts the term "is active" is not defined in the specification and that "is active" is not known to those with ordinary skill in the art. Applicant respectfully disagrees with the Examiner's assertion the term "is active" is neither defined in the specification nor known to those with ordinary skill in the art. Applicant respectfully asserts the term "is active" refers to while the key management system is running in memory, including both while the key management system is waiting for user input and while the key management system is processing user input. The Applicant's

assertion is supported by the enclosed "Declaration of Inventor Jameel Syed Under 37 CFR §1.132." As stated in the declaration, the term "is active" is known by those with at least ordinary skill in the art to be "while the application is running in memory," thus, no further definition is required in the specification.

Rejections under 35 U.S.C. §103

Claims 1-9 and 11-17 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,673,316 issued to Auerbach et al. (hereinafter "Auerbach"), in view of U.S. Patent No. 5,892,900 issued to Ginter et al. (hereinafter "Ginter I") and U.S. Patent No. 6,658,568 issued to Ginter et al. (hereinafter "Ginter II"). For the reasons set forth below, this rejection is respectfully traversed.

Amended independent claims 1 and 17 recite, in part, "a key management system providing process logic for key management system initialization located on the server comprising: a memory storing data in an n-tuple within the key management system, wherein the n-tuple comprises a key name field, a key value field, and a key type field." The Examiner has attempted to equate the document part and control (DC) parts, as well as the bill of materials (BOM) disclosed in Auerbach with n-tuples. (*See* Office Action dated October 24, 2005 at pages 7 and 8). These associations are improper as neither the BOM nor the DC parts have the structure or content of the n-tuple as recited in the claims.

The encrypted document parts disclosed by Auerbach contain material (*e.g.,* text, images, executable files, etc.) for purchase. The encrypted control parts disclosed by Auerbach contain the metadata needed to support the functions of the cryptographic envelope (*e.g.,* a price matrix, fingerprinting instructions, watermarking instructions, etc.). (*See* Auberbach at column 4, lines 3-18 and lines 25-42). However, Auerbach does not

contemplate using the DC parts to store an encryption key or information regarding an encryption key. In contrast, an n-tuple, as recited in the claims, is associated with a single encryption key, and includes the key name, the value of the key, and the type of the key. As the DC parts have neither the structure nor the content of the n-tuple, the DC parts are not and cannot be equivalent to the n-tuple as recited in the claims.

The BOM disclosed by Auerbach is used to ensure the authenticity of a cryptographic envelope. The BOM has two parts: a list of parts and a digital signature. The list of parts contains both the part name and a hashing value of the part. (*See* Auerbach at column 5, lines 13-35 and at Figure 3). However, as is the case with the DC parts, Auerbach does not contemplate using the BOM to store an encryption key or information regarding an encryption key. In contrast, an n-tuple, as recited in the claims, is associated with a single key, and includes the key name, the value of the key, and the type of the key. As the BOM has neither the structure nor the content of the n-tuple, the BOM is not and cannot be equivalent to the n-tuple as recited in the claims.

Both Ginter I and Ginter II disclose methods and systems for secure, automated transaction processing for use in electronic commerce over a network. (*See* Ginter I at abstract). However, like Auerbach, neither Ginter I nor Ginter II discloses the structure and content of an n-tuple as recited in amended independent claims 1 and 17. Thus, neither Ginter I nor Ginter II discloses what Auerbach lacks.

Auerbach, Ginter I, and Ginter II, whether viewed separately or in combination fail to teach or suggest each and every limitation of amended independent claims 1 and 17. Thus, amended independent claims 1 and 17 are patentable over Auerbach, Ginter I, and Ginter II. Claims 2-9 and 11-16 depend, either directly or indirectly, from amended claim 1

and thus are allowable for at least the same reasons. Accordingly, withdrawal of this rejection is respectfully requested.

Claims 18-20 and 22-35 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Auerbach in view of U.S. Patent No. 6,757,903 issued to Havemose (hereinafter "Havemose"). By way of this reply, claim 24 has been cancelled and thus the rejection is moot as to that claim. As for the remaining claims, for the reasons set forth below, this rejection is respectfully traversed.

Amended independent claims 18, 34, and 35 recite, in part, "combining data into a n-tuple comprising a key name field, a key value field, and a key type field." As discussed above the Examiner has attempted to equate this limitation with the document part and control (DC) parts, as well as the bill of materials (BOM) disclosed in Auerbach, with n-tuples. (*See* Office Action dated October 24, 2005 at pages 7 and 8). As discussed above, as neither the DC parts nor the BOM have the same structure and contents of a n-tuple, the DC parts and the BOM cannot be an n-tuple as recited in the claims. Havemose, like Auerbach, is completely silent regarding the structure and content of an n-tuple, and thus does not and cannot disclose what Auerbach lacks.

Auerbach and Havemose, whether viewed separately or in combination, fail to teach or suggest each and every limitation of amended independent claims 18, 34, and 35. Thus, independent claims 18, 34, and 35 are patentable over Auerbach and Havemose. Claims 19, 20, 22, 23, and 25-35 depend, either directly or indirectly, from claim 18 and are allowable for at least the same reasons. Accordingly, withdrawal of this rejection is respectfully requested.

Applicant asserts Havemose is non-analogous art. Havemose is directed towards an object driven software architecture that allows objects written in any programming language running on any operating system or hardware to communicate with any other object. (*See* Havemose at Abstract). In contrast, the claims are directed towards a network system for encryption key management. Applicant asserts one skilled in the art attempting to build a network encryption key management system would not look towards Havemose as a reference. Accordingly, Havemose is non-analogous art and withdrawal of this rejection is respectfully requested.

Applicant respectfully asserts that there is no motivation to combine the teachings of Auerbach with the teachings of Havemose. To properly combine references, the teaching or suggestion to make the claimed combination and the reasonable expectation of success must *both* be found in the prior art, *not* in Applicant's disclosure. *In re Vaeck*, 947 F.2d 488 (Fed. Cir. 1991) (emphasis added). Further, the mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. *In re Mills*, 916 F.2d 680 (Fed. Cir. 1990). In other words, there must be some objective reason to combine the teachings of the reasons. *Ex parte Levengood*, 28 USPQ2d 1300 (Bd. Pat. App. & Inter. 1993).

As discussed above, Havemose teaches an object driven software architecture that allows objects of varying types to communicate. In contrast, Auerbach teaches a method and apparatus to create, distribute, sell and control access to digital documents using secure cryptographic envelopes involving keys. The Examiner asserts it would be obvious to combine the teachings of Auerbach and Havemose in order to efficiently distribute dynamic objects. (*See* Office Action dated October 24, 2005 at pages 8 and 9). Applicant respectfully

asserts such a combination would not be obvious as Havemose is completely silent regarding encryption keys and encryption key initialization. Any motivation to combine the references is unrealistic.

A complete study of Havemose and Auerbach confirms that, regardless of whether the teachings of Havemose and Auerbach can be combined, there is no suggestion or motivation set forth in either Havemose or Auerbach to combine the teaching of these references. Absent such a suggestion or motivation, the teachings of Havemose and Auerbach cannot be conveniently combined to render the claimed invention obvious. Accordingly, withdrawal of this rejection is respectfully requested.

Claim 27 is indirectly dependent on claim 18. Amended claim 27 recites, in part, "tagging the secret token to associate it with an application, wherein the tag comprises the application's name." The Examiner has attempted to equate this limitation with cryptographic envelopes as disclosed by Auerbach. (*See* Office Action dated October 24, 2005 at page 8). This association is improper as the tagging process enables the key management system to serve multiple applications by effectively linking encryption keys to the corresponding application. (*See* Published Specification at paragraph [0041]). Applicant acknowledges the cryptographic envelopes disclosed by Auerbach are implemented using computer code and that cryptographic envelopes are executables, subroutines, modules or object components that can be manipulated and thus require a tag for definition. However, the tag disclosed in Auerbach is not associated with linking an encryption key to an application and thus is not and cannot be equivalent to the tagging process as recited in the claims. Havemose, like Auerbach, is completely silent regarding the tagging process as

recited in the claims as thus does not teach or suggest what Auerbach lacks. Accordingly, withdrawal of this rejection is respectfully requested.
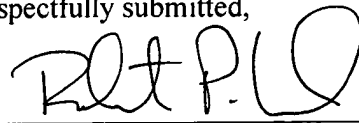
Conclusion

Applicant believes this reply is fully responsive to all outstanding issues and places this application in condition for allowance. If this belief is incorrect, or other issues arise, the Examiner is encouraged to contact the undersigned or his associates at the telephone number listed below. Please apply any charges not covered, or any credits, to Deposit Account 50-0591 (Reference Number 09469/010001).

Dated: January 24, 2006   Respectfully submitted,

By _____

Robert P. Lord
Registration No.: 46,479
OSHA · LIANG LLP
1221 McKinney St., Suite 2800
Houston, Texas 77010
(713) 228-8600
(713) 228-8778 (Fax)
Attorney for Applicant

Attachments – Declaration Under 37 CFR §1.132